Secret Data Hiding in Encrypted Compressed Video Bit streams for Privacy Info Protection

Pradeep Rajagopalan

Department of Electrical and Electronic Engineering

Easwari Engineering College, Anna University, Chennai, Tamilnadu, India

Abstract - This paper presents the encryption of compressed video bit streams and hiding privacy information to protect videos during transmission or cloud storage. Digital video sometimes needs to be stored and processed in an encrypted format to maintain security and privacy. Here, data hiding directly in the encrypted version of H.264/AVC video stream is approached, which includes the following three parts. By analyzing the property of H.264/AVC codec, the code words of intra prediction modes, the code words of motion vector differences, and the code words of residual coefficients are encrypted with stream ciphers. Then, a data hider may embed additional data in the encrypted domain by using wrapping technique, without knowing the original video content. The paper results shows that used methods provides better performance inerms of computation efficiency, high data security and video quality after decryption. The parameters such as RMSE, PSNR, CC are evaluated to measure its efficiency.

Index terms – H.264 Compression, chaos encryption, Bit wrapping based data hiding.

I. INTRODUCTION

It is widely used in medical and military imagery for secret data communication. The system uses the h.264 video encoding techniques for low bandwidth video transferring progress. In existing, pixel difference expansion based RDH is the spatial domain process to conceal secret text messages within a cover image. The data hiding involves histogram adjustment to reduce overflow and underflow error and adjacent pixels are subtracted to determine the differences values. Then difference will be either incremented or decremented based on message bits. This technique produces the spatial distortion leads to degrade an image quality and it is less compatible and complex one. This will be overcome by the method of least significant bit replacement algorithm. In Vacating room after encryption, the secret messages are concealed into encrypted domain by replacement of some pixel intensities. This spatial domain technique distorts an image quality wherever the secret message bits were hidden. With the consideration of these problems, the system proposes the reserve room approach with lifting wavelet transformation for preserving an image quality and improve the security of transmission. The technique lifting wavelet decomposes an image into frequency subbands which contains approximation and detailed coefficients. The system will reserve the coefficients from detailed components which have texture, edge and region boundary. It is insensible region for human visual system. In addition with this approach, chaos crypto system, adaptive least significant bit replacement will be used for image encryption and message embedding. Data recovery is the reverse process of the encryption and embedding to get lossless extracted image and messages. The simulated result shows performance of the used methodologies interms of metrics evaluation such as mean square error, peak signal to noise ratio and correlation coefficients.

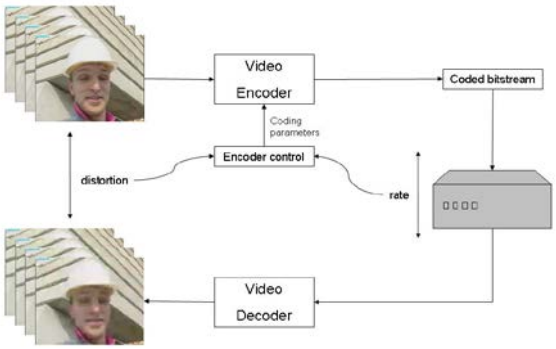
II. PROPOSED MODELS

In this section, a novel scheme of data hiding in the encrypted version of H.264/AVC videos is presented, which includes three parts, i.e., H.264/AVC video encryption, data embedding and data extraction. The content owner encrypts the original H.264/AVC video stream using standard stream ciphers with encryption keys to produce an encrypted video stream. Then, the data-hider (e.g., a cloud server) can embed the additional data into the encrypted video stream by using bit wrapping method, without knowing the original video content. At the receiver end, the hidden data extraction can be accomplished either in encrypted or in decrypted version.

After the compression process the encoded bit streams are going to encrypted using chaos encryption method.

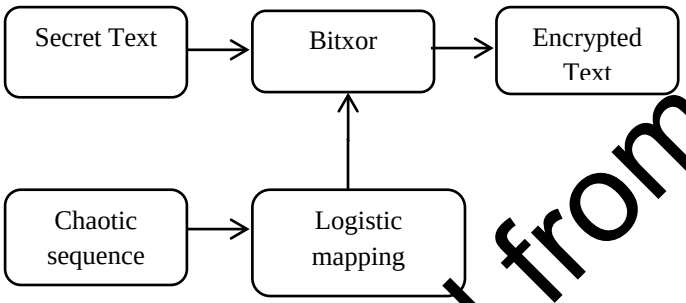
An H.264/AVC video encryption scheme with good performance including security, efficiency, and format compliance is proposed. By analyzing the property of H.264/AVC codec, three sensitive parts (i.e., IPMs, MVDs, and residual coefficients) are encrypted with stream ciphers. The proposed encryption algorithm is

performed not during H.264/AVC encoding but in the H.264/AVC compressed domain. In this case, the bit stream will be modified directly.



Secret Data Encryption

It is process of scrambling original information into unknown form using either symmetric or asymmetric key standard. Here it is one of the advanced encryption standard called chaos crypto system used. It encrypts the original image pixel values with encryption key value generated from chaotic sequence with threshold function by bitxor operation.



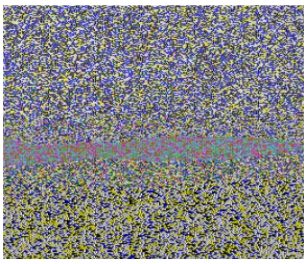
Here logistic map is used for generation of chaotic map sequence. It is very useful to transmit the secret image through unsecure channel securely which prevents data hacking. The chaotic systems are defined on a complex or real number space called as boundary continuous space. The chaotic sequence will be defined by, $C_{n+1}= U^* C_n*(1-C_n)$ and encrypted pixel form defined by

$$E = \text{bitxor}(P, C_{n+1})$$

Video Frames Encryption

The compressed bit streams are encrypted using bitxor operation. Then the encrypted text was hidden in the encrypted compressed bit streams. The below diagram shows the video frames and compressed bit frames.

Input frames



Encrypted Frames

Bit Wrapping

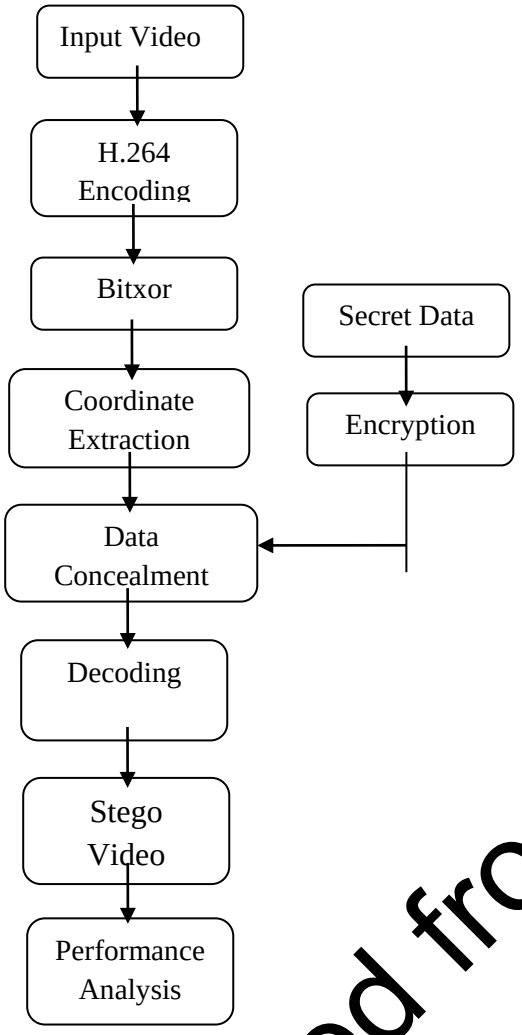
The process of bit wrapping method is to hide the encrypted secret data into the encrypted bit stream in the form of compression. The objective of steganography is a method of embedding additional information into the digital contents that is undetectable to listeners. We are investigating its embedding, detecting, and coding techniques. The idea behind the LSB algorithm is to insert the bits of the hidden message into the least significant bits of the pixels. As the application domain of embedding data in digital multimedia sources becomes broaden, several terms are used by various groups of researchers, including steganography, digital watermarking, and data hiding. The most frequently used steganography method is the technique of LSB substitution. In a gray-level image, every pixel consists of 8-bits. One pixel can hence display 28=256 variations. The weighting configuration of an 8-bit number is illustrated. The basic concept of LSB substitution is to embed the confidential data at the right most bits (bits with the smallest weighting) so that the embedding procedure does not affect the original pixel value greatly. The mathematical representation for LSB method is: *x* represents the *i* th pixel value of the stego-image, *i x* represents that of the original cover-image, and *i m* represents the decimal value of the *i* th block in confidential data. The number of LSBs to be substituted is denoted as k. The extraction process is to copy the k-rightmost bits directly. Mathematically the extracted message is represented as:

Hence, a simple permutation of the extracted *i m* gives us the original confidential data. This method is easy and straightforward. However, when the capacity is greatly increased, the image quality decreases a lot and hence a suspected stego-image results. Furthermore, the confidential data might be easily stolen by simply extracting the k-rightmost bits directly.

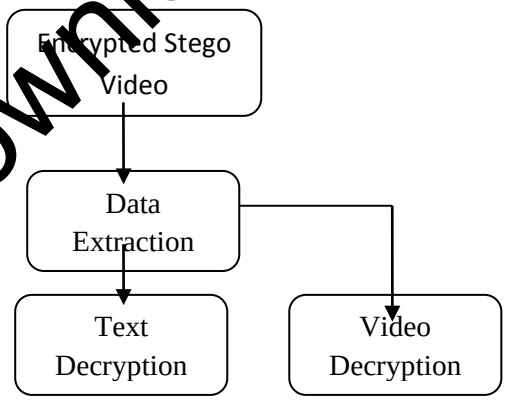
A 8-bit gray scale image matrix consisting m × n pixels and a secret message consisting of k bits. The first bit of message is embedded into the LSB of the first pixel and the second bit of message is embedded into the second pixel and so on. The resultant Stego-image which holds the secret message is also a 8-bit gray scale image and difference between the cover image and the Stego-image is not visually perceptible. The quality of the image, however degrades with the increase in number of LSBs. This hiding process will introduce the error between input and output image and it is determined by mean square error and Peak signal to noise ratio determines the image quality.

Process Flow:

Embedding



Extraction



Experimental Results

The performance of used methodology will be evaluated with different amount of characters on natural images. Here the metrics such as Mean square Error, PSNR and Correlation measured. Correlation = 0.8963 and PSNR = 43.78db.

CONCLUSION

The paper presented that protection of Video quality and hidden data during transmission based on approach of H.264 encoding and chaotic crypto system with bit wrapping based data concealment. Here, h.264 encoding method is used for compress the video frames effectively and chaos encryption was used as to protect image contents. This system was generated the stego video with less error under maximum data hiding capacity. It was better compatible approach and flexibility with better efficiency rather than prior methods

REFERENCES

[1] W. J. Lu, A. Varna, and M. Wu, "Secure video processing: Problems and challenges," in Proc. IEEE Int. Conf. Acoust., Speech, Signal Processing, Prague, Czech Republic, May 2011, pp. 5856–5859.
[2] B. Zhao, W. D. Kou, and H. Li, "Effective watermarking scheme in the encrypted domain for buyer-seller watermarking protocol," Inf. Sci., vol. 180, no. 23, pp. 4672–4684, 2010.
[3] W. Puech, M. Chaumont, and O. Strauss, "A reversible data hiding method for encrypted images," Proc. SPIE, vol. 6819, pp. 68191E-1–68191E-9, Jan. 2008
[4] X. P. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.
[5] W. Hong, T. S. Chen, and H. Y. Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Process. Lett., vol. 19, no. 4, pp. 199–202, Apr. 2012.
[6] X. P. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012
[7] K. D. Ma, W. M. Zhang, X. F. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553–562, Mar. 2013.